— EXHIBIT A —

2021 WL 4129202
Only the Westlaw citation is currently available.
United States District Court, D. South Carolina, Columbia Division.

Brady O'Leary, on behalf of himself and all others similarly situated, Plaintiff,

v.

TrustedID, Inc., Defendant.

C/A No. 3:20-cv-02702-SAL
|
Filed 09/09/2021

OPINION & ORDER

Sherri A. Lydon United States District Judge

***1** This matter is before the court on Defendant TrustedID, Inc.'s ("Defendant") Motion to Dismiss Plaintiff Brady O'Leary's ("Plaintiff") First Amended Complaint ("Motion to Dismiss") and Plaintiff's Motion to Remand or Determine Subject Matter Jurisdiction ("Motion to Remand"). [ECF Nos. 20, 44.] For the reasons set forth below, the court denies Plaintiff's Motion to Remand and grants Defendant's Motion to Dismiss.

BACKGROUND

This matter surrounds Defendant's "Look Up Tool"—an online tool created following the 2017 Equifax, Inc. ("Equifax") data breach.[1] The tool provided a mechanism for individuals to determine "whether they were 'impacted' by Equifax's data breach." [ECF No. 20, Am. Compl. at ¶ 10.] To use the tool, an individual would visit Defendant's website (https://trustedidpremier.com) and enter six digits of his/her social security number. *Id.* at ¶¶ 10–11. In return, the individual would receive a message stating whether the individual's data was or was not impacted by the Equifax breach. *Id.* at ¶ 11.

In this case, Plaintiff used the Look Up Tool in 2019—two years after the data breach—and learned that his data was "not impacted" by the breach. *Id.* He thereafter filed this action against Defendant in the South Carolina Court of Common Pleas, alleging the Look Up Tool's access requirement violates South Carolina's Financial Identity Fraud and Identity Theft Protection Act, S.C. Code Ann. § 37-20-110 *et seq.* ("SCITPA") and constitutes a common law invasion of privacy. [ECF No. 1-1.] On July 22, 2020, Defendant removed the action to this court on the basis of 28 U.S.C. § 1332(d), the Class Action Fairness Act. [ECF No. 1.]

After removal, Defendant moved to dismiss Plaintiff's Complaint, and Plaintiff filed his Amended Complaint.[2] [ECF Nos. 15, 20.] Plaintiff reasserted his statutory cause of action and the common law invasion of privacy claim, and he added a common law negligence cause of action. [ECF No. 20, Am. Compl.] Defendant moved to dismiss the Amended Complaint on October 23, 2020. [ECF No. 29.] Plaintiff responded to the Motion to Dismiss on November 20, 2020, and Defendant submitted a reply on December 10, 2020. [ECF Nos. 32, 37.] On August 10, 2021, the court issued a notice of hearing, setting the Motion to Dismiss for a September 7, 2021 hearing. [ECF No. 43.]

On August 23, 2021, Plaintiff filed the Motion to Remand. [ECF No. 44.] The court issued a text order directing the parties to be prepared to argue the remand issue at the September 7, 2021 hearing. [ECF No. 45.] Defendant filed its response in opposition to the Motion to Remand on the morning of September 7, 2021. [ECF No. 46.] The parties presented their arguments on both motions at the 2:00 PM hearing. [ECF No. 47.] With both motions fully briefed and heard, they are ripe for resolution by the court.

STANDARDS

I. Article III Standing's Injury-in-Fact Requirement: Motion to Remand.

***2** Jurisdiction in federal courts is limited to those cases where there is a "case" or "controversy" within the meaning of Article III. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559–60 (1992). In that regard, "standing is an essential and unchanging part of the case-or-controversy requirement of Article III." *Id.* at 560; *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) ("Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy."). It contains three elements: "The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo*, 136 S. Ct. at 1547.

As to the first element, a plaintiff must have "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.' " *Id.* at 1548 (citing *Lujan*, 504 U.S. at 560). An injury is particularized when it affect[s] the plaintiff in a personal and individual way.' " *Id.* (citing *Lujan*, 504 U.S. at n.1). An injury is concrete when it is " '*de facto*'; that is, it [ ] actually exist[s]." *Id.* (citing Black's Law Dictionary 479 (9th ed. 2009)).

Standing is so important that it may be raised at any time and by any party, including the court on its own initiative. *See Arbaugh v. Y&H Corp.*, 546 U.S. 500, 506 (2006) ("The objection that a federal court lacks subject-matter jurisdiction ... may be raised by a party, or by a court on its own initiative, at any stage in the litigation, even after trial and the entry of judgment."); *Hodges v. Abraham*, 300 F.3d 432, 443 (4th Cir. 2002) ("[S]tanding to sue is a jurisdictional issue of constitutional dimensions, and it may be raised and addressed for the first time on appeal."). And while "[t]he party invoking federal jurisdiction bears the burden of establishing [the] elements," "each element must be supported ... "with the manner and degree of evidence required at the successive stages of the litigation." *Lujan*, 5 U.S. at 561.

II. Rule 12(b)(6): Motion to Dismiss.

A party may move to dismiss a complaint based on its "failure to state a claim upon which relief may be granted." Fed. R. Civ. P. 12(b)(6). "The purpose of a Rule 12(b)(6) motion is to test the sufficiency of a complaint." *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (4th Cir. 1999). To survive a Rule 12(b)(6) motion, a complaint must have "enough facts to state a claim to relief that is plausible on its face," *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007), and contain more than "an unadorned, the-defendant-unlawfully-harmed-me accusation," *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In considering a motion to dismiss for failure to state a claim, a plaintiff's well-pled allegations are taken as true, and the complaint and all reasonable inferences are liberally construed in the plaintiff's favor. *Mylan Labs., Inc. v. Matkari*, 7 F.3d 1130, 1134 (4th Cir. 1993).

DISCUSSION

Before the court addresses the merits of Defendant's Motion to Dismiss, it must satisfy itself that it has subject-matter jurisdiction over this case. If it does not, it cannot reach the merits of Defendant's Motion. If it does, the case may proceed so long as the court remains satisfied that the requirements of Article III are met.

I. Motion to Remand Analysis.

Just over one year after Defendant removed[3] this case to federal court, Plaintiff filed a Motion to Remand. [ECF No. 44.] Therein, Plaintiff concedes that the requirements for jurisdiction pursuant to the Class Action Fairness Act are met, but argues that "the notice of removal makes no reference to the 'irreducible constitutional minimum' of Article III standing." *Id.* at pp.1–2. Pointing to the United States Supreme Court's June 25, 2021 opinion in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), Plaintiff asks the court to "inquire before reaching the merits into whether it has subject matter jurisdiction." *Id.* at p.2. At the same time, Plaintiff notes that he is "tak[ing] no position as to whether or not [the court] has jurisdiction." *Id.* Plaintiff submits, however, that if the court decides subject-matter jurisdiction is lacking, it must remand the case. *Id.* at p.3 (citing 28 U.S.C. § 1447(c)).

***3** In response, Defendant argues that *Ramirez* does not apply to this case, it properly removed the case based on the allegations in Plaintiff's Complaint, and there is no contradiction if the court finds Plaintiff's Complaint alleges a concrete injury and then dismisses for failure to adequately plead damages for a specific cause of action. [ECF No. 46.] The court agrees with Defendant.

Before reaching *Ramirez*, however, it is important to set forth some well-established principles regarding Article III's standing requirement. First, the general rule: To have standing to sue in federal court, a plaintiff must have suffered an injury in fact, that is fairly traceable to defendant's conduct, and that is likely to be redressed by a favorable decision. *Spokeo*, 136 S. Ct. at 1547. As the Seventh Circuit Court of Appeals recently recognized, "[t]he injury analysis often occurs at the pleading stage, where we are limited to the complaint's 'general factual allegations of injury resulting from the defendant's conduct' to evaluate standing." *Wadsworth v. Kross, Lieberman & Stone, Inc.*, No. 19-1400, 2021 WL 3877930, at *2 (7th Cir. Aug. 31, 2021) (citing *Lujan*, 504 U.S. at 561). The typical example is a challenge to subject-matter jurisdiction through a Defendant's Rule 12(b)(1) motion.

The present case differs procedurally from the typical example because this action was not filed in federal court in the first instance, and the plaintiff is not facing a defendant's Rule 12(b)(1) challenge. Instead, the case was removed to this court, and Plaintiff is challenging whether his own pleading (and arguably Defendant's notice of removal) satisfies the injury-in-fact requirement such that Defendant can keep this case in federal court. This situation, while not the most common, is also not unprecedented. *See, e.g., Michaeli v. Kentfield Rehab. Hosp. Found.*, No. 21-cv-03035, 2021 WL 2817162 (N.D. Cal. July 7, 2021) (considering motion to remand based on lack of Article III standing following removal). Regardless, because this matter is in its early pleading stages, the court is left with the Complaint's "general factual allegations of injury" to evaluate standing. *Wadsworth*, 2021 WL 3877930, at *2.

With that general background in mind, the court will turn to the specifics of the parties' arguments. Plaintiff's remand question focuses solely on the first standing requirement —an injury in fact.[4] More specifically, the requirement that the injury be "concrete."[5] To that point, Plaintiff cites the recent United States Supreme Court case, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), suggesting that his Complaint may not state an injury in fact for standing purposes. [ECF No. 44.] Defendant responds that *Ramirez* does not apply to the present case because nowhere in Plaintiff's pleading does he allege a mere risk of future harm, which, according to Defendant, was the focus of the *Ramirez* decision. [ECF No. 46.]

Ramirez is a class action that went all the way to trial on a Fair Credit Reporting Act ("FCRA") claim. The plaintiffs in that case had alerts labeling them as potential criminals or terrorists placed on their credit files maintained by a credit reporting agency. Specifically, the "alerts" indicated that the individuals' names were potential matches to the names of terrorists, drug traffickers, and other serious criminals that appeared on a list maintained by the Office of Foreign Assets Control. Some plaintiffs had their credit report, including the "alert," transmitted to third parties. Others did not. On certiorari, the Supreme Court held that those individual plaintiffs who did not have their credit reports transmitted to third parties did not suffer a concrete injury in fact for purposes of Article III's standing requirement. *Ramirez*, 141 S. Ct. at 2208–12. Distinguishing between disseminated credit reports and non-disseminated credit reports, the Court stated: "There mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." *Id.* at 2210.

***4** The opinion also reaffirmed several established points from *Spokeo*. First, it confirmed that "physical harms and monetary harms" are "[t]he most obvious [ ] traditional tangible harms" that can qualify as concrete injuries for purposes of Article III. *Id.* at 2204. Second, it confirmed that "[v]arious intangible harms can also be concrete," including "reputational harms, disclosure of private information, and intrusion upon seclusion," as well as "harms specified by the Constitution itself." *Id.* And third, it reiterated that standing does not exist simply because there is an alleged procedural violation of a statute. *Id.* at 2205; *see also id.* ("As Judge Katsas has rightly stated, 'we cannot treat an injury as 'concrete' for Article III purposes based only on Congress's say-so.' " (citing *Trichell v. Midland Credit Mgmt.*, 964 F.3d 990, 999 n.2 (11th Cir. 2020))). "Only those plaintiffs who have been concretely harmed by a defendant's statutory violation may sue that private defendant over the violation in federal court."[6] *Id.* Thus, for purposes of this court's analysis, *Ramirez* simply reminds it that if there is no concrete harm, there is no standing. *See id.* at 2214.

With *Ramirez*'s (and *Spokeo*'s) guiding principles in mind, the court turns to assessing whether there are sufficient allegations of a concrete harm in Plaintiff's pleading to pass the Article III standing threshold at this early stage of the case.[7] All of Plaintiff's claims flow from the same basic allegations: Equifax suffered a data breach in 2017; Defendant created a website that allows individuals to input six digits of their SSN to learn whether their data was compromised in the breach; Plaintiff used the website; the website failed to require any other information; the website's access requirements violated the SCITPA, resulted in an invasion of privacy, and served as negligent conduct by Defendant. Plaintiff contends that he had to enter his private information to "learn if he had been impacted by the breach," and the "arrangement [between Equifax and Defendant was ... an attempt to offload Equifax's affirmative data breach notification burden onto the consumer." Am. Compl. at ¶ 11 & n.1. In terms of the putative class, Plaintiff submits that "the claims ... arise from Defendant's failure to properly safeguard the personal information of Plaintiff and Class members." *Id.* at ¶ 26. The harm allegations, while perhaps scarce, certainly suggest that Plaintiff is claiming to have suffered some damage as a result of Defendant's actions. And Plaintiff seemingly concedes that the harm or injury suffered is the same for all three causes of action.[8]

The question then is whether these scarce allegations are enough to identify a concrete harm. In answering this question, let's start with what Plaintiff has not alleged in terms of harm. Plaintiff has not specifically alleged the common concrete harms—physical injury or monetary loss. He also has not alleged emotional injury. He doesn't seem to allege reputational harm. But has he alleged another intangible harm? Defendant argues "yes."

***5** Defendant submits that at this early pleading stage, Plaintiff's Complaint alleges an invasion of privacy or "intrusion upon seclusion," as used in *Ramirez*, as the alleged harm. [ECF No. 46 at p.5.] In that regard, Defendant notes the distinction between invasion of privacy as an alleged harm and invasion of privacy as a stand-alone common law cause of action. [ECF No. 46 at p.5.] And, even looking to *Ramirez*, we see that the Court did not require the harm alleged to be an "exact duplicate," of a "traditionally recognized" tort. 141 S. Ct. at 2209. Stated differently, Plaintiff's pleading alleges that he suffered an invasion of privacy, *i.e.*, harm, for purposes of the SCITPA cause of action, the invasion of privacy cause of action, and the negligence cause of action—it is the invasion itself that constitutes the alleged injury in fact. *See Ramones v. Experian Info. Sols., LLC et al.*, No. 19-cv-62949, 2021 WL 4050874, at *3 (S.D. Fla. Sept. 4, 2021) ("[A] plaintiff need not plead every element of a cause of action to establish a concrete injury.").

In accordance with the foregoing, the court concludes that Plaintiff's pleading alleges an intangible concrete *harm* in the manner of an invasion of privacy. This is enough to give the court subject-matter jurisdiction at this early stage of the case. That is not to say, however, that Plaintiff's invasion of privacy *claim* is sufficiently pleaded to survive a motion to dismiss. This takes us to the next question: Does Plaintiff's Amended Complaint survive Defendant's Motion to Dismiss?

II. Motion to Dismiss Analysis.

Defendant moves to dismiss all three of Plaintiff's claims. [ECF No. 29.] First, Defendant argues Plaintiff's allegations fit squarely into three exceptions to S.C. Code Ann. § 37-20-180's prohibition on the use of social security numbers to access a website. *Id.* at pp.4–9. Second, Defendant argues the tort claims must be dismissed due to Plaintiff's failure to allege cognizable damages. *Id.* at pp.9–12. Third, Defendant argues Plaintiff fails to plead other requisite elements of an invasion of privacy claim. *Id.* at pp.13–16. And finally, Defendant submits that Plaintiff has not alleged a legally cognizable duty to support his negligence claim. *Id.* at pp.16–19. With one exception limited to the invasion of privacy claim, Plaintiff opposes all of Defendant's arguments. [ECF No. 32.] The court, accordingly, addresses each argument in turn below.

A. SCITPA Exceptions.

Plaintiff's SCITPA claim relies on S.C. Code Ann. § 37-20-180, which is titled "Restrictions on publication and use of social security numbers; exceptions." He alleges Defendant violated subsection (A)(4) when it required Plaintiff to use six digits of his social security number to access the Look Up Tool. Am. Compl. at ¶¶ 29–35. The relevant portion of section 37-20-180 provides:

> Except as provided in subsection (B), a person may not ... require a consumer to use his social security number or a portion of it containing six digits or more to access an Internet web site, unless a password or unique personal identification number or other authentication devise is also required to access the Internet web site.

S.C. Code Ann. § 37-20-180(A)(4). Because Defendant's website did not require "a password or unique personal identification number or other authentication devise" in conjunction with the six-digit social security number, Plaintiff alleges it runs afoul of the statute. Am. Compl. at ¶ 21.

Defendant, acknowledging for the sake of the present Motion that Plaintiff has alleged a situation where a consumer uses six digits of his social security number to access a website, seeks dismissal of the claim. Defendant's arguments rely on the "[e]xcept as provided in subsection (B)" language in section 37-20-180(A)(4). Subsection (B) plainly provides that "[t]his section *does not apply*" to 10 enumerated scenarios. S.C. Code Ann. § 37-20-180(B). In this case, Defendant seeks dismissal based on the three subsection (B) exceptions. Specifically, Defendant argues subsection (A)(4) does not apply:

> ***6** (3) "to the opening of an account or the provision of or payment for a product or service authorized by a consumer;"
>
> (4) "to the collection, use, or release of a social security number to investigate or prevent fraud ...;"
>
> and

(7) "to a financial institution as defined in the Gramm-Leach-Bliley Act"—all of which are applicable to Plaintiff's allegations. S.C. Code Ann. § 37-20-180(B)(3), (4), (7).

First, Defendant argues it qualifies as a "financial institution as defined in the Gramm-Leah-Bliley Act" because it, as a "wholly owned subsidiary of Equifax," provides "financial, investment, or economic advisory services." [ECF No. 29-1 at pp.5–7]; *see also* S.C. Code Ann. § 37-20-180(B)(7). Defendant points to Plaintiff's allegation that Defendant "markets itself as an 'identity theft protection service,' offering free and paid products for that purpose." [ECF No. 29-1 at p.7]; Am. Compl. at ¶ 7. Second, Defendant argues it used the six digits of Plaintiff's social security number for "the provision of ... a ... service authorized by a consumer." S.C. Code Ann. § 37-20-180(B)(3); [ECF No. 29-1 at pp.7–8.] It contends that Plaintiff's allegations establish that he visited the website and entered the six digits of his social security number to determine whether his information had been impacted by the Equifax data breach. Am. Compl. at ¶¶ 11–12. Because the social security number was used to provide Plaintiff a service he authorized, Defendant argues it is exempt from the statute. And finally, Defendant argues that the Look Up Tool used the partial social security number to "to investigate or prevent fraud." S.C. Code Ann. § 37-20-180(B)(4); [ECF No. 29-1 at pp.8–9.] Defendant directs the court to Plaintiff's allegation that he used the tool to "confirm whether [his] personal information was ... acquired by an unauthorized person[.]" Am. Compl. at ¶ 12. Thus, Defendant contends that even if the court finds only one of the exceptions applicable, Plaintiff's claim must be dismissed.

Plaintiff responds generally that the statutory exceptions are affirmative defenses, meaning they may only be considered as bases for dismissal when "all facts necessary to the affirmative defense clearly appear[ ] on the face of the complaint." [ECF No. 32 at p.7 (citing *Goodman v. Praxair, Inc.*, 494 F.3d 458, 464 (4th Cir. 2007).] Here, Plaintiff contends the necessary facts do not appear on the face of his pleading and dismissal is not warranted. As to the first exception, Plaintiff argues Defendant fails to show that it, as opposed to Equifax, engages in any financial activities as defined by the Gramm-Leach-Bliley Act ("GLBA"). [ECF No. 32 at pp.8–10.] With the second exception, Plaintiff submits that his use of the website should not be considered "voluntary," given that the information provided was "information Equifax was legally required to provide." *Id.* at p.11. Finally, as to the third exception argued by Defendant, Plaintiff submits that Defendant did not undertake any investigation. Rather, it merely informed individuals whether or not their information was the subject of the data breach. *Id.* at pp.12–13.

***7** Neither side cites caselaw interpreting or applying S.C. Code Ann. § 37-20-180, and the court's independent research did not reveal any. In deciding this Motion, the court is left with the plain language of the statute and Plaintiff's allegations. *See Knotts v. S.C. Dep't of Nat. Resources*, 558 S.E.2d 511, 516 (S.C. 2002) ("If a statute's language is plain, unambiguous, and conveys a clear meaning 'the rules of statutory interpretation are not needed and the court has no right to impose another meaning.' " (citation omitted)); *Thompson v. Richland Cty. Sch. Dist. One*, No. 3:17-cv-510, 2018 WL 2676159, at *3 (D.S.C. June 5, 2018) (finding language of South Carolina's Whistleblower statute clear and unambiguous and granting motion for judgment on the pleadings for failure to state a claim). Moreover, even assuming (without deciding) Plaintiff is correct that the exceptions found in subsection (B) are affirmative defenses, the court may still grant the motion if it finds that all necessary facts appear on the face of the complaint. *Goodman*, 494 F.3d at 464. Having considered the parties' positions, Plaintiff's Amended Complaint, and the statutory language, the court agrees with Defendant that the SCITPA claim must be dismissed. Each exception is addressed below.

1. "Financial Institution."

At the outset, the court is not convinced that there is sufficient information appearing on the face of Plaintiff's pleading to establish that Defendant is or is not a "financial institution" under the GLBA. Moreover, the court is not willing to conclude that Defendant qualifies as a "financial institution" as a matter of law at this stage of the case.

The GLBA defines "financial institution" as an entity "engaging in financial activities as described in Section 4(k) of [the Bank Holding Company Act of 1956 ("BHCA")]." 15 U.S.C. § 1609(3)(A). It is considered a "broad" definition given that the BHCA lists activities that "shall be considered to be financial in nature" to include "[p]roviding financial, investment, or economic advisory services." 12 U.S.C. § 1843(k)(4)(C); *see also FTC v. AmeriDebt, Inc.*, 343 F. Supp. 2d 451, 457 (D. Md. 2004) (recognizing "financial institution" "includes several entities not traditionally recognized as financial institutions"). In keeping with the broad reading, and as noted by Defendant in this case, courts have recognized credit bureau services as "financial institutions" under the GLBA. *See, e.g., Trans*

Union LLC v. FTC, 295 F.3d 42, 48–49 (D.C. Cir. 2002) (concluding the Federal Trade Commission "permissibly determined that Trans Union, which provides [credit bureau services] ... comes within the GLBA's definition of a 'financial institution' ").

Here, Plaintiff's Amended Complaint alleges that Defendant "markets itself as a protector of *identity* theft." Am. Compl. at ¶ 1 (emphasis added); *see also id.* at ¶ 7 ("Defendant ... markets itself as an 'identity theft protection service,' offering free and paid products for that purpose."), ¶ 8 ("Defendant itself provides no 'financial services' to consumers[.]").[9] Identity theft may, and often does, include a financial component. But in this case, whether the "identity theft" protection tools offered by Defendant have a financial, investment, or economic advisory component, remains an open question. The court is not ruling out the possibility that Defendant may qualify as a "financial institution" as defined by the GLBA, but it is not willing to so find at this early juncture and on the limited record available to it.

2. Investigating Fraud.

***8** In line with the court's conclusion on the "financial institution" exception, the court declines to rule that the pleading firmly establishes the third exception on which Defendant relies—investigating fraud.

The relevant portion of the exception reads: "This section does not apply... to the collection, *use*, or release of a social security number to investigate or prevent fraud[.]" S.C. Code Ann. § 37-20-180(B)(4) (emphasis added). In their briefing, the parties take differing approaches on "who" must be investigating fraud for the exception to apply. Defendant argues *Plaintiff* was investigating potential fraud when he admittedly used the Look Up Tool to confirm whether his information was compromised in the Equifax data breach. [ECF No. 29-1 at p.8.] Thus, it submits the exception must apply. Plaintiff, in contrast, argues the Look Up Tool did not investigate anything. Instead, it simply informed him and others of "a theft that had already occurred." [ECF No. 32 at p.12.]

Based on the court's reading of the exception, both Plaintiff and Defendant may be right. If an entity, such as Defendant, "collect[s]" or "use[s] ... a social security number to investigate or prevent fraud," the exception would apply. S.C. Code Ann. § 37-20-180(B)(4). Similarly, if an individual, such as Plaintiff, used a website to "release [his] social security number to investigate or prevent fraud," it seems the exception would apply. But the "actor" question is not the dispositive one for purposes of this action. The court need only decide whether the allegations of the Amended Complaint qualify as "*investigating* ... fraud."[10] S.C. Code Ann. § 37-20-180(B)(4) (emphasis added). Without additional information on how the Look Up Tool worked to confirm the information provided to the users, the court is not willing to conclude at this point that it used the social security numbers to *investigate* fraud. Thus, the court declines to dismiss the pleading based on this exception.

3. Service Authorized by Consumer.

The court is persuaded, however, by Defendant's section 37-20-180(B)(3) argument: That the Look Up Tool constitutes "the provision of ... a ... service authorized by a consumer." In the words of Defendant's counsel during the hearing, "Plaintiff pleaded himself into the exception."

Plaintiff's pleading states that "in order to learn if he had been impacted by the breach, Plaintiff entered the required information, including six (6) digits of his Social Security number" into the Look Up Tool. Am. Compl. at ¶ 11. "In exchange for and after giving this information to Defendant, Plaintiff was told he was 'not impacted' by Equifax's data breach." *Id.* According to Defendant, these allegations establish the social security number was used to provide a service to Plaintiff. The court agrees.

In construing and applying subsection (B)(3), this court is tasked with giving the words therein "their plain and ordinary meaning without resort to subtle or forced construction to limit or expand its operation." *Hitachi Data Sys. Corp. v. Leatherman*, 420 S.E.2d 843, 846 (S.C. 1992). "Where a word is not defined in a statue," such as the word "service" here,[11] the court looks "to the usual dictionary meaning to supply its meaning." *Lee v. Thermal Eng'g Corp.*, 572 S.E.2d 298, 303 (S.C. Ct. App. 2002). Merriam-Webster defines "service" in various ways to include "help, use, benefit" and "useful labor that does not produce a tangible commodity[.]" *Service*, Merriam-Webster Dictionary (online ed. 2021).

***9** In this case, there is no question that the Look Up Tool, as alleged by Plaintiff, provided "help," a "benefit," or even "useful labor" in that it informed inquiring individuals whether their information had been impacted by Equifax's data breach. Plaintiff's own response in opposition to the Motion recognizes that this information is of great value.

[ECF No. 32 at p.11.] Thus, the court concludes that the Look Up Tool provided a "service" to the public, including Plaintiff. The question then is whether the allegations of the Amended Complaint establish that Defendant's provision of that service was "*authorized* by [the] consumer." S.C. Code Ann. § 37-20-180(B)(3) (emphasis added).

Plaintiff's argument in this regard focuses on whether his actions were "voluntary." [ECF No. 32 at p.11.] According to Plaintiff, the statutory exception does not apply because *Equifax* had an "unambiguous statutory duty to notify South Carolinians whose data was stolen" and *Defendant's* Look Up Tool left consumers with no choice at all. *Id.* Consumers could "give TrustedID the information it asked for or live with not knowing whether Equifax had allowed his personal information to be stolen." *Id.* This argument misses the mark.

This lawsuit is not determining whether *Defendant's* Look Up Tool satisfied *Equifax's* data breach notice requirements. Equifax is not a party to this case. The only question for this court is whether the access requirements for *Defendant's* website violate section 37-20-180(A)(4). If Plaintiff's allegations establish that he "authorized" the use of his social security number to learn whether his persona information was impacted by Equifax's data breach, the exception applies and the claim must be dismissed. The court need not look at what notice Equifax did or did not send.

Plaintiff's Amended Complaint unambiguously states: "[T]o learn if he had been impacted by the breach, Plaintiff entered the required information, including six (6) digits of his Social Security number into Trusted ID's website," and in "exchange for ... this information ..., Plaintiff was told he was 'not impacted' by Equifax's data breach." Am. Compl. at ¶ 11. These allegations establish: (1) Plaintiff wanted to know whether his information was impacted by Equifax's data breach; (2) He went to Defendant's website to invoke the service offered; and (3) In "exchange for" this information, he inputted his social security number. Thus, Plaintiff authorized Defendant to use his social security number to tell him whether his information was impacted by the Equifax data breach. Plaintiff received exactly what he wanted to know and what Defendant said it would provide. Plaintiff's Amended Complaint alleges all requirements in S.C. Code Ann. § 37-20-180(B)(3), the exception applies, and Defendant is entitled to dismissal of SCITPA claim.[12]

B. Tort Claims.

***10** In addition to the SCITPA claim, Plaintiff asserts two common law tort claims: (1) invasion of privacy and (2) negligence. Defendant argues Plaintiff fails to allege damages associated with the two tort claims and fails to allege all required elements of the two claims. Plaintiff responds that, to the extent required, he has alleged damage, and he plausibly alleges all elements of his negligence and invasion of privacy claims. The arguments related to each claim are addressed below.

1. Invasion of Privacy.

Starting with the invasion of privacy claim, Plaintiff alleges he has a right to keep his social security number private; the right is evidenced by the SCITPA and "elsewhere," Defendant "chose to require Plaintiff to come to Defendant; instead of affirmatively notifying Plaintiff" of the Equifax breach, the "intrusion was intentional;" and "Defendant knew or should have known ... South Carolina's prohibitions against requiring such information." Am. Compl. at ¶¶ 36–46. Defendant submits that these allegations fail to state a claim for any of the three recognized theories of invasion of privacy in South Carolina. [ECF No. 29-1 at pp.13–16.] The court agrees.

The South Carolina Supreme Court has identified three theories that may give rise to a cause of action for invasion of privacy:

> [1] The unwarranted appropriation or exploitation of one's personality, [2] the publicizing of one's private affairs with which the public has no legitimate concern, or [3] the wrongful intrusion into one's private activities, in such manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities.

Meetze v. Associated Press, 95 S.E.2d 606, 608 (S.C. 1956) (quotation omitted); *see also Sloan v. S.C. Dep't of Pub. Safety*, 586 S.E.2d 108, 110 (S.C. 2003) (outlining "three separate and distinct causes of action for invasion of privacy"). In this case, Plaintiff concedes that he is not proceeding on the second theory—wrongful publicizing of private affairs. [ECF No. 32 at p.19.] Thus, the court focuses its attention on the first and third theories.

a. Wrongful Appropriation.

The first theory—wrongful appropriation of personality—"involves the intentional, *unconsented* use of the plaintiff's name, likeness, or identity by the defendant for his own

benefit." *Sloan*, 586 S.E.2d at 110 (emphasis added). "The gist of the action is the violation of the plaintiff's exclusive right at common law to publicize and profit from his name, likeness, and other aspects of personal identity." *Id.* As recently recognized by the Honorable David C. Norton, "while publicity is not explicitly stated as an element per se, it is still a fundamental requirement of the cause of action for wrongful appropriation of personality." *J.R. v. Walgreens Boots Alliance, Inc.*, 470 F. Supp. 3d 534, 551 (D.S.C. 2020), *appeal docketed*, No. 20-1767 (4th Cir. July 14, 2020).

Defendant argues Plaintiff fails to state a wrongful appropriation claim for three reasons: (1) Plaintiff fails to allege his social security number was publicized to the public; (2) Plaintiff affirmatively alleges he consented to Defendant's use of his social security number; and (3) Plaintiff fails to allege Defendant used his "name, likeness, or identity" for its "own benefit." [ECF No. 29-1 at pp.11, 13–14.] Plaintiff opposes all three arguments, arguing he has alleged information sharing with affiliates and the extent of that information sharing is not yet known, [ECF No. 32 at p.19]; consent is "immaterial" because it is an affirmative defense, *id.* at p.20; and damages are not an element of a tort claim for invasion of privacy, *id.* at p.19. The court agrees with Defendant.

***11** First, as to the publication requirement, Plaintiff's pleading alleges only that "upon information and belief, Defendant's collection or use [of] six digits of Plaintiff's Social Security number was not 'internal' to Trusted ID, but *shared with* Equifax." Am. Compl. at ¶ 17 (emphasis added). Nowhere does he allege that Defendant publicized this information to the public at large. *See J.R.*, 470 F. Supp. 3d at 551–52 ("Even accepting as true the factual allegation that non-pharmacy Walgreen Co. employees can access ... plaintiffs' PII, the court fails to see how this access constitutes publicity as a matter of law."). The "sharing" alleged here can be equated to the access available to employees in the J.R. case recently decided by Judge Norton: "The fact that [Equifax] can access plaintiffs' PII does not mean that plaintiffs' PII is communicated to the public at large." *Id.* at 552. Because "publicity is required in a wrongful appropriation of personality claim" and Plaintiff fails to allege such publicity, the claim is subject to dismissal. *Id.*; *see also Holloman v. Life Ins. Co. of Va.*, 7 S.E.2d 169, 171 (S.C. 1940) (finding claim failed because life insurance policy did not publicize the plaintiff's name; "issuance of a small life insurance policy seems to fall short of publicity").

Second, Defendant is correct that to state a claim for wrongful appropriation, Plaintiff must allege an "unconsented use." *Sloan*, 586 S.E.2d at 110. Plaintiff's Amended Complaint identifies only one plausible use of his personal information —to notify him whether he was or was not impacted by the Equifax data breach. Am. Compl. at ¶¶ 10, 11. The pleading makes it clear that Plaintiff, wanting to know whether his information was impacted by the Equifax data breach, went to Defendant's website, submitted his information, and obtained the results. Plaintiff's speculative allegation that "Defendant had additional purposes in [obtaining his SSN]" does not equate to an allegation of "unconsented use." For this reason, Plaintiff has not stated a claim for wrongful appropriation.

And third, Defendant is correct that Plaintiff's pleading fails to allege that Defendant used his personal identifying information for its own benefit. Again, Plaintiff makes an allegation "upon information and belief" that "Defendant's collection or use ... of Plaintiff's Social Security number was not 'internal' to Trusted ID, but shared with Equifax." Am. Compl. at ¶ 17. This allegation of sharing does not equate to an allegation of use for Defendant's own benefit.

For these three reasons, the court grants Defendant's Motion as to the wrongful appropriation invasion of privacy claim.

b. Wrongful Intrusion.

The second theory—wrongful intrusion into private affairs —requires a plaintiff to demonstrate: (1) an intrusion; (2) into that which is private; (3) which is substantial and unreasonable; and (4) intentional. *Morris v. Ocwen Loan Servicing, LLC*, No. 0:16-cv-1772, 2017 WL 1035944, at *5 (D.S.C. Mar. 17, 2017). Generally, an "intrusion may consist of watching, spying, prying, besetting, overhearing, or other similar conduct." *Id.* at n.2 (citing *Snakenberg v. Hartford Cas. Ins. Co.*, 383 S.E.2d 2, 6 (S.C. Ct. App. 1989)). Moreover, "[w]hen a plaintiff bases an action for invasion of privacy on 'intrusion' alone, bringing forth no evidence of public disclosure, it is incumbent upon him to show a blatant and shocking disregard for his rights, and serious mental or physical injury or humiliation to himself resulting therefrom." *Id.* at n.4 (citing *Rycroft v. Gaddy*, 314 S.E.2d 39, 43 (S.C. Ct. App. 1984)).

Defendant argues this theory fails for three reasons: (1) Plaintiff does not allege any serious mental or physical injury from inputting his social security number into the Look Up

Tool and obtaining the results; (2) Plaintiff fails to allege any facts showing a shocking disregard for his rights; and (3) Plaintiff concedes he gave his social security number to Defendant, Defendant did not "intrude." [ECF No. 29-1 at pp.11, 15–16.] Plaintiff disputes these arguments, as well. He contends the giving of the information was not voluntary; Defendant acted intentionally in obtaining the information; and he plausibly alleges a blatant and shocking disregard for his rights. [ECF No. 32 at pp.20–21.] The court again agrees with Defendant, but declines to reach the damages argument.

***12** First, the court agrees with Defendant that the Amended Complaint fails to state any conduct by Defendant that could be construed as "watching, spying, prying, besetting, overhearing, or other similar conduct." *Morris,* 2017 WL 1035944, at *5 n.2 (citing *Snakenberg*, 383 S.E.2d at 6). There simply is no intrusion alleged here. Defendant created a website that allowed individuals to input their social security numbers to learn whether their information was impacted by the Equifax data breach. Defendant did not require anyone to use the website. Defendant did not use any tricks or tactics to obtain the social security numbers. Plaintiff's own pleading makes it clear that he wanted to know whether he was impacted by the breach, he knew he could do so by accessing the website, and he entered the social security number when requested. Accordingly, Plaintiff has not alleged an intrusion, let alone one that is "substantial and unreasonable." *Id.* at *5.

Second, much like with the SCITPA claim, Plaintiff's reliance on the alleged actions of Equifax to support a "blatant and shocking disregard of his rights" by Defendant misses the mark. Plaintiff argues that "a company who (a) calls itself an 'identity theft protection service' (b) responds to its parent company's failure to secure consumers' private identifying information by (c) creating a website that requires ... more private identifying information ... to (d) simply [ ] receive the notice it was the consumers' legal right to receive ... would seem to 'plausibly' suggest a 'blatant and shocking disregard' for those consumers' rights." [ECF No. 32 at pp.20–21.] The court cannot agree. Simply creating a website that allows individuals to enter their information to determine whether or not their personal information was or was not impacted by another entity's data breach is not sufficient to state a claim of invasion of privacy. *Land v. Green Tree Servicing, LLC*, No. 8:14-cv-1165, 2014 WL 5527854, at *7 (D.S.C. Oct. 31, 2014). If Equifax was required to give notice and it did not, that is an issue that must be addressed with (or a claim that must be asserted against) Equifax.

For the foregoing reasons, the court finds Plaintiff has not state a claim for invasion of privacy based on wrongful intrusion into private affairs.

2. Negligence.

Plaintiff's final claim is one for negligence. Plaintiff alleges Defendant undertook to "shift the burden of notifying consumers in South Carolina whether they were impacted by the Equifax data breach to those consumers" and assumed that duty to do so "non-negligently and in compliance" with the law. Am. Compl. at ¶ 48. According to Plaintiff, Defendant "breached its duty by collecting information in a manner violative of federal and South Carolina law." *Id.* at ¶ 50. Plaintiff states generally that he was "damaged." *Id.* at ¶ 51.

Defendant argues the negligence claim must be dismissed because Plaintiff (1) fails to allege any cognizable damages, [ECF No. 29-1 at p.12] and (2) fails to allege a duty owed by Defendant, *id.* at pp.16–19. Plaintiff's opposition arguments are tied together; first, he claims the duty alleged is one that Defendant undertook voluntarily in creating the Look Up Tool, and second, "it is enough for him to allege simply that he in fact suffered damages because of [Defendant's] disregard of the legal duty it assumed." [ECF No. 32 at pp.16–18.] Having thoroughly considered the parties' arguments, the court must again agree with Defendant that the negligence claim is subject to dismissal.

Briefly as to the duty issue, the best the court can determine is that Plaintiff is attempting to argue as follows: Equifax had a duty to notify consumers if their information was compromised by the data breach; in creating the Look Up Tool, Defendant assumed Equifax's duty to notify; and Defendant breached the assumed duty when it asked individuals to submit six digits of their social security numbers to access the information without additional protections. Even if Plaintiff adequately alleged the aforementioned scenario (and he did not), Plaintiff still faces the problem that his information was not compromised. If his information admittedly was not compromised, how would Equifax (or Defendant) have had a duty to notify Plaintiff of anything? Further, as noted by Defendant, Plaintiff has not alleged any "*physical* harm resulting from" Defendant's alleged negligence in performing its undertaking. *See Wright v. PRG Real Estate Mgmt., Inc.*, 826 S.E.2d 285, 291 (S.C. 2019) (citing Restatement (Second) of Torts § 323 (1965) for proposition that "[o]ne who undertakes ... to render services to another ... is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care

to perform his undertaking"). But, in any event, the lack of damages alleged in the Amended Complaint is also fatal to Plaintiff's negligence claim.

***13** In South Carolina, to establish a cause of action for negligence, a plaintiff must plead and prove four elements: (1) a duty of care; (2) breach of the duty by negligent act or omission; (3) resulting damages to the plaintiff; and (4) the damages were the proximate result of the breach. *See Thomasko v. Poole*, 561 S.E.2d 597, 599 (S.C. 2002). "Generally, under South Carolina law, the damages element requires a plaintiff to establish physical injury or property damage;" "mere annoyance, inconvenience, or discomfort a plaintiff may suffer" is not enough. *Babb v. Lee Cty. Landfill S.C., LLC*, 747 S.E.2d 468, 481 (S.C. 2013). And because this action is in federal court, the damages element must be pleaded with the same specificity required by Rule 8, FRCP. *Stephens v. United States*, No. 0:16-cv-149, 2017 WL 217965, at *4 (D.S.C. Jan. 19, 2017). Stated simply, the allegation that Plaintiff was "damaged" does not meet that standard.

CONCLUSION

For the foregoing reasons, Plaintiff Brady O'Leary's Motion to Remand, ECF No. 44, is **DENIED**, and Defendant TrustedID, Inc.'s Motion to Dismiss the Amended Complaint, ECF No. 29, is **GRANTED**.

IT IS SO ORDERED.

All Citations

Slip Copy, 2021 WL 4129202

Footnotes

1 Defendant is a wholly owned subsidiary of Equifax, Inc. [ECF Nos. 3, 20 at ¶ 8; *see also* ¶ 18 ("Equifax is a separate jural person from Trusted ID.")]

2 The Honorable Mary Geiger Lewis entered an order mooting the first motion to dismiss on October 20, 2020. [ECF No. 28.]

3 Defendant's notice of removal alleges subject-matter jurisdiction exists pursuant to 28 U.S.C. § 1332(d). [ECF No. 1 at ¶¶ 18–37.]

4 Neither party challenges the other two requirements for standing, traceability and redressability.

5 Again, neither party challenges the requirement that the plaintiff's alleged injury be particularized.

6 The statute at issue in this case is not federal. It is a state statute that is part of South Carolina's Consumer Protection Code. The court assumes, however, that the Supreme Court's analysis regarding the concrete injury requirement applies in the same way.

7 Since the notice of removal, Plaintiff has filed an Amended Complaint. [ECF No. 20.] The main distinction between the first complaint and the operative complaint is the addition of a negligence cause of action in the Amended Complaint. [*Compare* ECF No. 1-1, *with* ECF No. 20.] The factual allegations remain substantively the same. Thus, whether the court assesses the specific allegations of the Complaint or the Amended Complaint, its answer will be the same.

8 Neither the Complaint nor the Amended Complaint make any distinctions between the "harm" suffered in relation to the three causes of action as a result of Defendant's actions. At the hearing, Plaintiff described the harm as intentionally taking personal identifying information and monetizing it in some way.

9 The court declines to consider Defendant's Terms of Use. [ECF No. 29-1 at p.6 (arguing the Terms of Use were incorporated by reference into the Amended Complaint).] A court reviewing a Rule 12(b)(6) motion "may ... consider documents incorporated into the complaint by reference ... so long as they are integral to the complaint and authentic." *United States ex rel. Oberg v. Penn. Higher Educ. Assistance Agency*, 745 F.3d 131, 136 (4th Cir. 2014) (citation and quotation marks omitted). The Terms of Use, while perhaps integral to Defendant's argument, are not integral to Plaintiff's complaint.

10 There seems to be no dispute here that Defendant's Look Up Tool was not used for "*preventing* fraud." S.C. Code Ann. § 37-20-180(B)(4) (emphasis added). The fraud, if any, had already occurred by the time the Look Up Tool was created.

11 During the hearing, Plaintiff pointed out that the word "services" is defined by S.C. Code Ann. § 37-2-105(3) as "(a) work, labor, and other personal services, (b) privileges with respect to transportation, hotel and restaurant accommodations, education, entertainment, recreation, physical culture, hospital accommodations, funerals, cemetery accommodations, and the like, and (c) insurance provided by a person other than the insurer." Plaintiff seemed to suggest that the website does not meet that definition. The problem for Plaintiff is that the definition appears in Chapter 2 of Title 37, which governs Credit Sales. The SCITPA exception uses the word "service" (as opposed to "services") and appears in Chapter 20 of

Title 37, Consumer Identity Theft Protection. Chapter 20 has its own definitions, which are found in S.C. Code Ann. § 37-20-110. The word "service" is not defined therein.

12 The court only briefly addresses Plaintiff's contention that "[t]o the extent Defendant's actions fit any exception ..., Plaintiff is informed and believes that Defendant had additional purposes in doing so that did not meet any exception under the statute." Am. Compl. at ¶ 16. This allegation does not present the court with any plausible theory of recovery. While the "plausibility standard is not akin to the probability requirement," it requires "more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)); *see also Twombly*, 550 U.S. at 570 (requiring a complaint to include "enough *facts* to state a claim to relief that is plausible on its face" (emphasis added)). This speculative allegation in the Amended Complaint cannot—and does not—save Plaintiff's claim from dismissal.

End of Document